

CLAIMS

- 1 1. A method of pro-actively refreshing credentials by an entity that maintains cre-
2 dentials, the method comprising the steps of:
- 3 a) storing in a memory, a profile collection having at least one credential profile,
4 each credential profile including a credential and related information;
- 5 b) causing the stored credential in the credential profile to be examined in accor-
6 dance with a refresh policy;
- 7 c) comparing at least one criterion of the refresh policy with the related informa-
8 tion to determine if the credential needs to be refreshed;
- 9 d) replacing the stored credential with a new credential in the credential profile if
10 the stored credential needs to be refreshed;
- 11 e) updating the related information of the new credential in the credential profile;
12 and
- 13 f) repeating the steps of c) – e) on a next credential profile in the profile collec-
14 tion.
- 1 2. The method of claim 1, wherein before step a), the method further comprises the
2 steps of:
- 3 determining if the credential profile for a needed credential exists; and if not, then
4 creating an empty credential profile;

5 gathering the credential;
6 storing the credential in the credential profile;
7 obtaining related information including resource constraints on the credential;
8 storing the information in the credential profile; and
9 repeating the steps if another credential profile needs to be created.

1 3. The method of claim 2, wherein the step of obtaining resource constraints is per-
2 formed by manual entry of a user.

1 4. The method of claim 2, wherein the step of obtaining resource constraints is de-
2 duced through access attempts.

1 5. The method of claim 2, wherein the step of obtaining resource constraints is ob-
2 tained from a directory.

1 6. The method of claim 2, wherein the step of obtaining resource constraints is ob-
2 tained from a resource server.

1 7. The method of claim 2, wherein the stored credential includes a public key iden-
2 tity credential.

- 1 8. The method of claim 2, wherein the stored credential includes a group member-
2 ship credential.
- 1 9. The method of claim 2, wherein the stored credential includes a group non-
2 membership credential.
- 1 10. The method of claim 2, wherein the stored credential includes a non-revocation
2 credential.
- 1 11. The method of claim 2, wherein the stored resource constraints include a recency
2 requirement.
- 1 12. The method of claim 2, wherein the stored resource constraints include a trust
2 level.
- 1 13. The method of claim 2, wherein the stored resource constraints include a maxi-
2 mum credential chain length.
- 1 14. The method of claim 1, wherein the related information includes storing informa-
2 tion on a credential identifier.

- 1 15. The method of claim 1, the related information includes storing information on
2 when the credential was issued.
- 1 16. The method of claim 1, the related information includes storing information on
2 when the credential was last used for a resource access.
- 1 17. The method of claim 1, the related information includes storing information on
2 which resource the credential was last used.
- 1 18. The method of claim 1, includes refreshing credentials that are older than a certain
2 time period.
- 1 19. The method of claim 1, includes refreshing credentials that were last used within a
2 certain time period.
- 1 20. The method of claim 1, includes refreshing credentials that are older than an asso-
2 ciated recency requirement.
- 1 21. The method of claim 1, includes refreshing credentials that are predicted to be
2 used in a next session.

1 22. A processor executable medium having instructions contained therein which when
2 executed by a processor causes the processor to execute a method of pro-actively
3 refreshing credentials by an entity that maintains credentials, the method com-
4 prising the steps of:

- 5 a) storing in a memory, a profile collection having at least one credential profile,
6 each credential profile including a credential and related information;
- 7 b) causing the stored credential in the credential profile to be examined in accor-
8 dance with a refresh policy;
- 9 c) comparing at least one criterion of the refresh policy with the related informa-
10 tion to determine if the credential needs to be refreshed;
- 11 d) replacing the stored credential with a new credential in the credential profile if
12 the stored credential needs to be refreshed;
- 13 e) updating the related information of the new credential in the credential profile;
14 and
- 15 f) repeating the steps of c) – e) on a next credential profile in the profile collec-
16 tion.

1 23. The processor executable medium of claim 22, wherein before step a), the method
2 further comprises:
3 determining if the credential profile for a needed credential exists; and if not, then

4 creating an empty credential profile;
5 gathering the credential;
6 storing the credential in the credential profile;
7 obtaining related information including resource constraints on the credential;
8 storing the information in the credential profile; and
9 repeating the steps if another credential profile needs to be created.

1 24. The processor executable medium of claim 23, wherein the step of obtaining re-
2 source constraints is performed by manual entry of a user.

1 25. The processor executable medium of claim 23, wherein the step of obtaining re-
2 source constraints is deduced through access attempts.

1 26. The processor executable medium of claim 23, wherein the step of obtaining re-
2 source constraints is obtained from a directory.

1 27. The processor executable medium of claim 23, wherein the step of obtaining re-
2 source constraints is obtained from a resource server.

1 28. The processor executable medium of claim 23, wherein the stored credential in-
2 cludes a public key identity credential.

1 29. The processor executable medium of claim 23, wherein the stored credential in-
2 cludes a group membership credential.

1 30. The processor executable medium of claim 23, wherein the stored credential in-
2 cludes a group non-membership credential.

1 31. The processor executable medium of claim 23, wherein the stored credential in-
2 cludes a non-revocation credential.

1 32. The processor executable medium of claim 23, wherein the stored resource con-
2 straints include a recency requirement.

1 33. The processor executable medium of claim 23, wherein the stored resource con-
2 straints include a trust level.

1 34. The processor executable medium of claim 23, wherein the stored resource con-
2 straints include a maximum credential chain length.

- 1 35. The processor executable medium of claim 22, the related information includes
2 storing information on a credential identifier.
- 1 36. The processor executable medium of claim 22, the related information includes
2 storing information on when the credential was issued.
- 1 37. The processor executable medium of claim 22, the related information includes
2 storing information on when the credential was last used for a resource access.
- 1 38. The processor executable medium of claim 22, the related information includes
2 storing information on which resource the credential was last used.
- 1 39. The processor executable medium of claim 22, includes refreshing credentials that
2 are older than a certain time period.
- 1 40. The processor executable medium of claim 22, includes refreshing credentials that
2 were last used within a certain time period.
- 1 41. The processor executable medium of claim 22, includes refreshing credentials that
2 are older than an associated recency requirement.

1 42. The processor executable medium of claim 22, includes refreshing credentials that
2 are predicted to be used in a next session.

1 43. A system for pro-actively refreshing credentials by an entity that maintains cre-
2 dentials, the system comprising:
3 a memory to store a profile collection having at least one credential profile, each
4 credential profile including a credential and related information;
5 a circuit to read the credential profile;
6 a refresh policy stored in the memory to determine if the credential needs to be re-
7 freshed using the related information, wherein the circuit replaces the stored cre-
8 dential with a new credential in the credential profile if the stored credential needs
9 to be refreshed and the circuit updates the related information of the new creden-
10 tial in the credential profile.

1 44. The system of claim 43, wherein system further comprises:
2 the circuit configured to determine if the credential profile for a needed credential
3 exist; and if not, then
4 the circuit configured to create an empty credential profile in the memory, the cir-
5 cuit further configured to gather the credential and store the credential in the cre-
6 dential profile, the circuit configured to obtain related information including re-

7 source constraints on the credential and store the information in the credential pro-
8 file.

1 45. The system as in claim 44, wherein the circuit is a processor.

1 46. The system of claim 44, wherein the resource constraints is obtained by manual
2 entry of a user.

1 47. The system of claim 44, wherein the resource constraints is deduced through ac-
2 cess attempts.

1 48. The system of claim 44, wherein the resource constraints is obtained from a di-
2 rectory.

1 49. The system of claim 44, wherein the resource constraints is obtained from a re-
2 source server.

1 50. The system of claim 44, wherein the stored credential includes a public key iden-
2 tity credential.

1 51. The system of claim 44, wherein the stored credential includes a group member-
2 ship credential.

1 52. The system of claim 44, wherein the stored credential includes a group non-
2 membership credential.

1 53. The system of claim 44, wherein the stored credential includes a non-revocation
2 credential.

1 54. The system of claim 44, wherein the stored resource constraints include a recency
2 requirement.

1 55. The system of claim 44, wherein the stored resource constraints include a trust
2 level.

1 56. The system of claim 44, wherein the stored resource constraints include a maxi-
2 mum credential chain length.

1 57. The system of claim 43, wherein the stored information includes a credential
2 identifier.

1 58. The system of claim 43, wherein the stored information includes when the cre-
2 dential was issued.

1 59. The system of claim 43, wherein the stored information includes when the cre-
2 dential was last used for a resource access.

1 60. The system of claim 43, wherein the stored information includes on which re-
2 source the credential was last used.

1 61. The system of claim 43, wherein the refresh policy refreshes credentials that are
2 older than a certain time period.

1 62. The system of claim 43, wherein the refresh policy refreshes credentials that were
2 last used within a certain time period.

1 63. The system of claim 43, wherein the refresh policy refreshes credentials that are
2 older than an associated recency requirement.

1 64. The system of claim 43, wherein the refresh policy refreshes credentials that are
2 predicted to be used in a next session.